ABSTRACT OF THE DISCLOSURE

An absolute public key cryptographic system and method that survives private key compromise and offers two-way communication security. It secures the confidentiality of the private-to-public side communications and also allows short keys to be used for mobile devices that have low processing power. The system uses keys with two or more components and encrypts a message into the same number of versions, and delivers to the destination with a small time gap, where the recipient performs certain mathematical operations on all these versions and obtains the original message. All the versions are necessary for decryption into the original message. Even a single version missing would produce a junk message for an eavesdropper. As an eavesdropper at an intermediary IP router can not have all the versions available, he can not deduce the original message even when he knows the private key. This is why the system is called absolute public key cryptography. The robustness against private key compromise is achieved by blinding the public key through adding a random number to each of its components before encryption. When the encryption process is complete the random number is discarded and the encrypted message versions are delivered to the recipient. The effect of blinding is neutralized by the actual intended recipient, who has all the encrypted message versions available. Robustness is also achieved another way, that is, by choosing the encrypting key such that each of its components has a common factor with Euler Totient Function of the key modulus and there is no common factor among all the components. This makes it harder for an eavesdropper to decrypt a single version of the message into the original message and thereby allows smaller keys to be used for mobile communications. Communication in both directions is secured by using two different key pairs, one for public-to-private-side and the other for private-to-public-side communications.